X-520-69-527

NASA TM X- 70699

ON THE AUTO AND CROSSCORRELATION OF PN SEQUENCES

JAMES C. MORAKIS

DECEMBER 1969

GSFC

GODDARD SPACE FLIGHT CENTER

GREENBELT, MARYLAND

X-520-69-527

ON THE AUTO AND CROSSCORRELATION OF PN SEQUENCES

James C. Morakis

December 1969

Goddard Space Flight Center
Greenbelt, Maryland

CONTENTS

ON THE AUTO AND CROSSCORRELATION OF PN SEQUENCES

James C. Morakis

ABSTRACT

The autocorrelation and crosscorrelation properties of pseudorandom (PN) sequences are analyzed by using some important properties of PN sequences. These properties make this discussion understandable without the need of linear algebraic approach. The analysis is followed by some experimental results.

ON THE AUTO AND CROSSCORRELATION OF PN SEQUENCES

Due to increasing interest in PN codes for applications in multiple user and or combat of multipath and others the author has decided to compile some of the already known and other recent developments on the correlation properties of PN coding schemes and their intercomparison. The basic linear PN code generation is discussed extensively in [1] and some of the important properties of PN codes will be repeated for convenience.

A maximal linear PN Sequence is defined as a sequence generated by a linear* feedback shift register m stages long such that the length of the sequence is the maximum possible for a constant m. It can be easily shown that if such a maximal sequence exists its length must be

$$L = 2^m - 1 .$$

Figure 1 demonstrates such a feedback shift register with h_i either 0 or 1 $h_i = 1$ means that there is a connection and $h_i = 0$ means that there is no connection ($h_0 = h_m = 1$ always). One can consider the contents of the shift register as the state of the shift register. If the state is known at time t_i then the next state is given by a relationship of the original state and the transition matrix A**.

The characteristic equation of the matrix A turns out to be [1]

$$P_A(x) = \sum_{i=0}^{m} h_i x^i \quad \text{with } h_i = 0, 1 \text{ and } h_0 = h_m = 1 .$$

* The only allowable logic is mod 2 which is an exculusive-or gate.

** See Apendix A for the exact form of A in terms of the h_i connections.

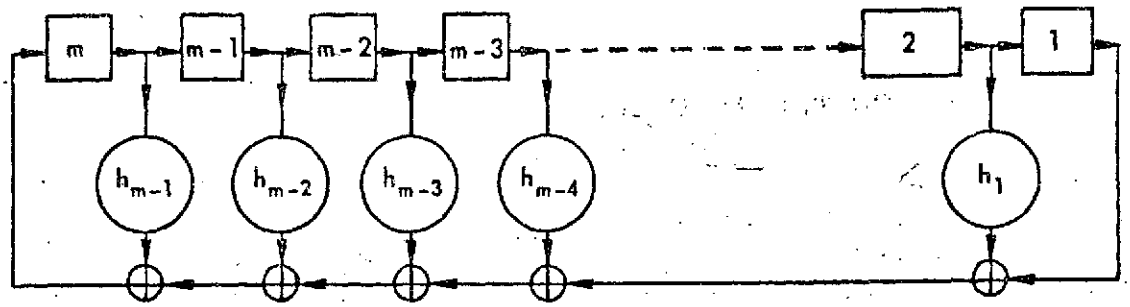

Figure 1–A Linear Feedback Shift Register

This polynomial is also called the generating polynomial of the sequence. If this polynomial is primitive then the sequence is maximal. This polynomial, just like any other polynomial of degree m, has m roots which might be designated as $\alpha, \alpha_1, \alpha_2 \ldots\ldots\ldots \alpha_{m-1}$. The knowledge of any one of the above m roots is sufficient because all the others can be represented as powers of the one chosen. Thus we can say that $P_A(x)$ has a root α. If a polynomial has a root β such that $\beta = \alpha^k$, k any integer, then that polynomial is either polynomial $P_A(x)$ or another primitive polynomial. The number of distinct maximal sequences that can be generated by an m-stage shift register is given by [1]

$$\frac{\phi(2^m - 1)}{m}$$

where $\phi(j)$ is the Euler phi function and it is equal to the number of integers prime to j but less than j. So if j is a prime $\phi(j) = j - 1$. Table 1 gives the number of maximal sequences the length L and other information for each m. Table 1 also gives a listing of the first few Mersenne primes which are defined as the m's which are prime such that $2^m - 1$ is also a prime. Obviously Mersenne primes result in large numbers of maximal sequences. To investigate the correlation properties of shift register generated sequences we must first discuss some pertinent properties. A sequence of period L can be viewed as a sequence of L states (or L n-dimensional vectors; $L = 2^n - 1$ for binary).

Property A. A maximal binary sequence will occupy all $2^n - 1$ non-zero states before it starts repeating.

Property B. (Balance property) The number of 1's in a maximal sequence exceeds the number of 0's by 1.

Thus the number of zeros of a maximal sequence is equal to $2^{n-1} - 1$ and the number of 1's is equal to 2^{n-1}.

Table 1

m	$L = 2^m - 1$	Prime factors of $2^m - 1$	$(2^m - 1)$	$\frac{(2^m - 1)}{n}$
2	3	3	2	1
3	7	7	6	2
4	15	$3 \cdot 5$	8	2
5	31	31	30	6
6	63	$3^2 \cdot 7$	36	6
7	127	127	126	18
8	255	$3 \cdot 5 \cdot 17$	128	16
9	511	$7 \cdot 73$	432	48
10	1023	$3 \cdot 11 \cdot 31$	600	60
11	2047	$23 \cdot 89$	1936	176
12	4095	$3^2 \cdot 5 \cdot 7 \cdot 13$	1728	144
13	8191	8191	8190	630
14	16383	$3 \cdot 43 \cdot 127$	10584	756
15	32767	$7 \cdot 31 \cdot 151$	27000	1800
16	65535	$5 \cdot 3 \cdot 17 \cdot 257$	32768	2048
17	131071	131071	131070	7710
18	262143	$3^3 \cdot 7 \cdot 19 \cdot 73$	139968	7776
19	524287	524287	524286	27594
20	1048575	$3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$	480000	24000

Mersenne Primes:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, ...

Property C. (The Shift-and-add property.)

When a maximal sequence is first shifted by t bits and then added to itself the resulting sequence is the same sequence delayed by some time t_1 i.e.

$$S_A(t) + s_A(t-k) = s_A(t-t_1) \text{ for } k \neq 0.$$

Property D. This is really a transformation process that applies to all binary waveforms. It facilitates the calculation of correlation by transforming multiplication into mod 2 addition. As a result of this transformation 1's in a binary sequence are transformed into 0's, the -1's are transformed into 1's and the correlation is given by

$$R_{S_A S_B} = \frac{\#\text{ of 0's in } S_C - \#\text{ of 1's in } S_C}{L} \quad (1)$$

where S_C is the sequence formed by adding S_A to S_B mod 2, bit by bit.

The above four concepts will enable us to arrive at some of the most important conclusions on the values of auto and crosscorrelation of linear PN sequences without becoming dazed by the complex maze of modern math which would normally be necessary for this purpose.

Auto-Correlation of a Linear Maximal PN Sequence

The goal is to evaluate

$$R_{S_A}(k) = \frac{1}{L} \sum_{j=1}^{L} S_A(t_j) \cdot S_A(t_j - k)$$

where the dimension of t and k is time in integer numbers of bits.

Application of the transformation D results in

$$R_{S_A}(k) = R_{S_A\ S_B}(k) = \frac{\#\ 0\text{'s in } S_C - \#\ 1\text{'s in } S_C}{L}$$

where

$$S_C = S_A(t) \oplus S_A(t-k)$$

for $k \neq 0$.

Application of property C results in

$$S_C = S_A(t) \oplus S_A(t-k) = S_A(t-t_1)$$

Thus S_C is the sequences S_A shifted by some delay t_1; by property A, $L = 2^n - 1$ and by property B

$$\#\ 0\text{'s} - \#\ 1\text{'s in } S_A(\ ) = -1$$

and $R_{S_A}(k) = -1/(2^n - 1)$ for $k \neq 0$; for $k = 0$

$$S_C = S_A(t) \oplus S_A(t) = 2\,S_A(t) = 0 \mod 2$$

thus S_C is the all zero sequence (# of 0's = L and # 1's = 0) and

$$R_{S_A}(0) = \frac{L}{L} = 1$$

as expected.

Cross Correlation of Linear Maximal PN Sequences

The cross correlation of two distinct linear maximal PN sequences S_A and S_B is given by equation (1) with

$$S_C = S_A(t) \oplus S_B(t - k) \quad \text{any } k$$

Unfortunately the shift and add property cannot be used here. Thus we cannot predict at this point the values taken by $R_{AB}(k)$ as a function of k. The literature is not helpful either in this respect; however some bounds* have been given. These bounds are very loose (i.e., the observed autocorrelation values are much less than the bound) except for a specific one derived by Gold [2] and applicable to only certain pairs of sequences. The results of this reference will now be stated and explained.

Let $P_A(x)$ and $P_B(x)$ be two primitive polynomials of degree m with roots α and β respectively and let T (an integer number) be

$$T = 2^{\frac{m+1}{2}} + 1 \quad \text{for } m \text{ odd}$$

and

$$T = 2^{\frac{m+2}{2}} + 1 \quad \text{for } m \text{ even}, \; m \not\equiv \bmod 4$$

if

$$\alpha = \beta^T$$

then

$$R_{AB}(k) \leq T / (2^n - 1)$$

This is the only tight crosscorrelation bound that is available at the present and, at the risk of being repetitious, it should be emphasized that this bound applies

* These are upperbounds on $R_{S_A S_B}(k)$ and imply that this R is less than a certain value (the bound).

only to a few chosen pairs of PN sequences. As an example consider m = 5, the number of maximal sequences is (from table 1) 6, the length is 31, and T = 9. If sequence S_B is chosen with generating polynomial $P_B(x)$ of root β, then choose sequence S_A corresponding to polynomial $P_A(x)$ whose root is $\alpha = \beta^9$; the correlation $R_{AB}(k)$ for any k will be equal to or less than 9/31 = .29. Notice that the roots of $P_A(x)$* are $\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}$, the roots of $P_B(x)$ are $\beta = \alpha^9$, $\beta^2 = \alpha^{18}$, $\beta^4 = \alpha^5$, $\beta^8 = \alpha^{10}$, $\beta^{16} = \alpha^{20}$ (five roots for each polynomial of degree 5). There are four more maximal sequences from the four polynomials

$$P_C(x),\ P_D(x),\ P_E(x),\ P_F(x)$$

the roots of $P_C(x)$ are $\gamma = \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}$

the roots of $P_D(x)$ are $\delta = \alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}$

the roots of $P_E(x)$ are $\epsilon = \alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}$

the roots of $P_F(x)$ are $\omega = \alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}$

Also notice that $\gamma^T = (\alpha^3)^T = \alpha^{27}$

thus $P_C(x)$ and $P_F(x)$ are also a pair of polynomials whose sequences exhibit the Gold bound. In a similar fashion we can find the remaining pairs which are P_B and P_D, P_D and P_A P_E and P_C and finally P_F and P_E.

Thus for any k

$$R_{DA}(k) \leq 9/31$$

$$R_{FC}(k) \leq 9/31$$

$$R_{EC}(k) \leq 9/31$$

$$R_{FE}(k) \leq 9/31$$

$$R_{BD}(k) \leq 9/31$$

*See Appendix B.

There are two unsolved problems here. The first problem is: What is the maximum crosscorrelation of the remaining 9 pairs such as the pairs (A,C), (A,E), (A,F), (B,C), (B,E), (B,F), (C,D), (D,E), (P,F). The second problem is what is the distribution of R_{AB} (k)?

Presently the answers to the above problem, are obtained by brute exhaustive simulation. Some shortcuts can be taken by using some of the theory, but the shortcuts simply mean less computer time. An exhaustive simulation was performed by the author with m = 7 and 11; the results for m = 7 are outlined in the next section.*

Experimental Results on the Crosscorrelation of Linear Maximal PN Sequences of m = 7

The eighteen PN sequences with m = 7 and L = 127 have been generated† and the crosscorrelation of each pair was found exhausively for all k (0 to 126). The results showed that for a certain group of pairs the crosscorrelation takes on a certain number of values with the same frequency. For example, for a certain group‡ which I shall call Group A the crosscorrelation took on the values -17 for 28 k's, 15 for 36 k's and -1 for 63 k's. The different groups and the crosscorrelation values have been tabulated in Table 3. It can be seen from Table 3 that there are three sets of crosscorrelation values. For certain pairs of sequences the crosscorrelation takes on the values -17, -1, 15 with the frequencies shown under Group A, for other pairs it takes on the values -41, -17, -9, -1, 7, 15, 23 with the frequencies shown under Group B and for pairs consisting of any sequence and its reverse the crosscorrelation taken on the values indicated by Group C.

Table 4 shows how 16 of the 18 sequences divide into Groups A and B when each of the eighteen sequences is the sequence being crosscorrelated (its reverse belongs to Group C). An explanation of this division into the two groups is given in Appendix C.

It can be shown§ that the grouping of the sequences as observed in Table 4 is strictly a function of the roots of the sequence generator polynomials♦.

---

† See Table 2 for identification of each sequence and its roots

‡ This group is the one that includes the α^{17} polynomial.

* The results for m =9, 10, 11, and 12 will be published soon.

§ See Appendix C

♦ The roots of the polynomials generating the sequence are referred to here as the roots of the sequence for the sake of brevity.

Table 2

The 18 Maximal sequences with m = 7 and the corresponding roots

Sequence number and corresponding root of generating polynomial	The complete set of roots satisfying the sequence (only exponents of α are shown)
1 - α	1, 2, 4, 8, 16, 22, 64
2 - α^{63}	63, 126, 125, 123, 119, 111, 95
3 - α^{3}	3, 6, 12, 24, 48, 96, 65
4 - $(\alpha^{3})^{63} = \alpha^{31}$	31, 62, 124, 121, 115, 103, 79
5 - α^{5}	5, 10, 20, 40, 80, 33, 66
6 - $(\alpha^{5})^{63} = \alpha^{61}$	47, 94, 61, 122, 117, 107, 87
7 - α^{7}	7, 14, 28, 56, 112, 97, 67
8 - $(\alpha^{7})^{63} = \alpha^{15}$	15, 30, 60, 120, 113, 99, 71
9 - α^{9}	9, 18, 36, 72, 17, 34, 68
10 - $(\alpha^{9})^{63} = \alpha^{59}$	55, 110, 92, 59, 118, 109, 91
11 - α^{11}	11, 22, 44, 88, 49, 98, 69
12 - $(\alpha^{11})^{63} = \alpha^{58}$	39, 78, 29, 58, 116, 105, 83
13 - α^{13}	13, 26, 52, 104, 81, 35, 70
14 - $(\alpha^{13})^{63} = \alpha^{57}$	23, 46, 92, 57, 114, 101, 75
15 - α^{19}	19, 38, 76, 25, 50, 100, 73
16 - $(\alpha^{19})^{63} = \alpha^{54}$	27, 54, 108, 89, 51, 102, 77
17 - α^{21}	21, 42, 84, 41, 82, 37, 74
18 - $(\alpha^{21})^{63} = \alpha^{53}$	43, 86, 45, 90, 53, 106, 85

Sequences numbered with odd numbers are taken from [3]; sequences whose number is even and next to an odd number are the corresponding reverse sequences, i.e., 2 is the reverse of 1, 12 is the reverse of 11, etc.

Table 3

Tabulation of Crosscorrelation values ($R \times 127$) and Corresponding Frequencies

$127\ R_{xy}(k)$	Frequency or # of t's		
	Group A	Group B	Group C
-41	0	1	0
-37	0	0	0
-33	0	0	0
-29	0	0	0
-25	0	0	0
-21	0	0	7
-17	28	14	7
-13	0	0	8
- 9	0	28	21
- 5	0	0	7
- 1	63	35	14
3	0	0	21
7	0	28	7
11	0	0	14
15	36	14	14
19	0	0	7
23	0	7	0
Total	127	127	127

Specifically if the root of a sequence is η then the sequences with η^{ℓ_A} belong to group A, the sequences with roots η^{ℓ_B} belong to Group B and the sequences with roots η^{ℓ_C} belong to Group C.

For

$$m = 7 \quad (L = 127)$$

$$\ell_A = 3, 5, 15, 9, 11, 39, 13, 23, 27, 43$$

$$\ell_B = 31, 47, 7, 55, 19, 21$$

and

$$\ell_C = 63$$

Note that for this case $9 \sim 17 \mod 127$ represents the Gold sequence, and 63 represents the reverse sequence.

It should be observed that the crosscorrelation is always an odd number. The reason is the fact that L (= 127) is odd, and the # of zeros plus the number of 1's must equal L while

$$L\,R_{ab} = \theta_{ab} = \#\text{ of 0's} - \#\text{ 1's} = 2(\#\text{ 0's}) - L \quad \text{odd QED}$$

Another observation is that the crosscorrelation in group C takes on values equal to 3 mod 4. This indicates that the number of zero's in the resulting sequence, $S_C = S_A \oplus S_B$ is always odd. (The crosscorrelation in group A is 3 mod 16 and for group B it is 3 mod 8.)*

The Correlation as a Random Variable

In view of the results of Table 3 the crosscorrelation of the three groups will be treated as a random variable. The reason for doing this is the following. Although Group A has the smallest maximum crosscorrelation Groups B and C seem to be more toward the center. First let us find the mean and variance of the autocorrelation if the autocorrelation is regarded as a random variable.

*See Reference [4].

Table 4
Correlation Groups for the 18 Sequences of m = 7

Part 1. If S_α is sequence #1 (reverse sequence is #2)
Group A = Sequence #'s 3, 5, 8, 9, 11, 12, 13, 14, 16, 18
Group B = Sequence #'s 4, 6, 7, 10, 15, 17

Part 2. If S_α is sequence #2 (reverse sequence is #1)
Group A = Sequence #'s 4, 6, 7, 10, 11, 12, 13, 14, 15, 17
Group B = Sequence #'s 3, 5, 8, 9, 16, 18

Part 3. If S_α is sequence #3 (reverse sequence is #4)
Group A = 5, 6, 8, 9, 11, 12, 13, 16, 18, 1
Group B = 7, 10, 13, 15, 17, 2

Part 4. If S_α is sequence #4 (reverse sequence is #3)
Group A = 5, 6, 7, 10, 11, 12, 14, 15, 17, 2
Group B = 8, 9, 13, 16, 18, 1

Part 5. If S_α is sequence #5 (reverse sequence is #6)
Group A = 8, 9, 10, 11, 14, 15, 18, 1, 3, 4
Group B = 7, 12, 13, 16, 17, 2

Part 6. If S_α is sequence #6 (reverse sequence is #5)
Group A = 7, 9, 10, 12, 13, 16, 17, 2, 3, 4
Group B = 8, 11, 14, 15, 18, 1,

Part 7. If S_α is sequence #7 (reverse sequence is #8)
Group A = 9, 8, 10, 12, 13, 15, 16, 17, 2, 4, 6
Group B = 11, 14, 18, 1, 3, 5

Part 8. If S_α is sequence #8 (reverse sequence is #7)
Group A = 9, 10, 11, 14, 15, 16, 18, 1, 3, 5, 7
Group B = 12, 13, 17, 2, 4, 6

Part 9. If S_α is sequence #9 (reverse sequence is #10)
Group A = 12, 13, 16, 18, 1, 3, 5, 6, 7, 8
Group B = 11, 14, 15, 17, 2, 4

Part 10. If S_α is sequence #10 (reverse sequence is #9)
Group A = 11, 14, 15, 17, 2, 4, 5, 6, 7, 8
Group B = 12, 13, 16, 18, 1, 3

Part 11. If S_α is sequence #11 (reverse sequence is #12)
Group A = 14, 15, 18, 1, 2, 3, 4, 5, 8, 10
Group B = 13, 16, 17, 6, 7, 9

Part 12. If S_α is sequence #12 (reverse sequence is #11)
Group A = 13, 16, 17, 1, 2, 3, 4, 6, 7, 9
Group B = 14, 15, 18, 5, 8, 10

Table 4 (continued)

Part 13. If S_a is sequence #13 (reverse sequence is #14)
Group A = 16, 17, 18, 1, 2, 3, 6, 7, 9, 12
Group B = 15, 4, 5, 8, 10, 11

Part 14. If S_a is sequence #14 (reverse sequence is #13)
Group A = 15, 17, 18, 1, 2, 4, 5, 8, 10, 11
Group B = 16, 3, 6, 7, 9, 12

Part 15. If S_a is sequence #15 (reverse sequence is #16)
Group A. = 17, 18, 2, 4, 5, 7, 8, 10, 11, 14
Group B. = 1, 3, 6, 9, 12, 13

Part 16. If S_a is sequence #16 (reverse sequence is #15)
Group A. = 17, 18, 1, 3, 6, 7, 8, 9, 12, 13
Group B. = 2, 4, 5, 10, 11, 14

Part 17. If S_a is sequence #17 (reverse sequence is #18)
Group A = 2, 4, 6, 7, 10, 12, 13, 14, 15, 16
Group B = 1, 3, 5, 8, 9, 11

Part 18. If S_a is sequence #18 (reverse sequence is #17)
Group A = 1, 3, 5, 8, 9, 11, 13, 14, 15, 16
Group B = 2, 4, 6, 7, 10, 12

*Group C has only the reverse sqeuence. The reverse pairs are (1, 2), (3, 4), (5, 6), (7, 8), (9, 10), (11, 12), (13, 14), (15, 16) and (17, 18).

Since its two values are 1 for $\tau = 0$ and -1 for the $2^m - 2$ cases where $\tau \neq 0$

$$\bar{\theta} = \left[\sum_i \theta_i f(\theta_i)\right] / (2^m - 1)$$

$$= [(2^m - 1)\,1 + (-1)(2^m - 2)]/(2^m - 1) = 1/(2^m - 1)$$

$$\bar{R} = \bar{\theta}/(2^m - 1) = 1/(2^m - 1)^2$$

$f(\theta_i)$ is the frequency of the i^{th} value of the random variable. The variance of $\hat{\theta}$ becomes:

$$\sigma_\theta^2 = \left[\sum_i \theta_i^2 \, f(\theta_i)\right] / (2^m - 1) - \bar{\theta}^2$$

$$= \frac{(2^m - 1)^2 + (-1)^2 (2^m - 2) - \bar{\theta}^2}{2^m - 1} = \frac{(2^m - 1)^2 + 2^m - 2 - 1/(2^m - 1)}{2^m - 1}$$

$$\sigma_R^2 = \sigma_\theta^2 / (2^m - 1)^2 = \frac{(2^m - 1)^2 + 2^m - 2 - 1/(2^m - 1)}{(2^m - 1)^3}$$

for the case $m = 7$, $2^m - 1 = 127$ and

$$\bar{\theta} = 1/127$$

and

$$\sigma_\theta = \sqrt{\frac{(127)^2 + 126 - 1/127}{127}} = 11.313358$$

and

$$\sigma_R = \frac{\sigma_\theta}{127} = .0891 \quad \sigma_R^2 = .00793$$

Similarly a simple calculation reveals that

$\overline{\theta^{(A)}} = 1/127$, $\overline{|\theta^{(A)}|} = 1079/127$, $= 8.496062$, $\sigma_\theta^{(A)} = 11.3133$

$\overline{\theta^{(B)}} = 1/127$, $\overline{|\theta^{(B)}|} = 1133/127 = 8.92$, $\sigma_\theta^{(B)} = 11.3133$ or $\sigma_\theta = \sqrt{\frac{16255}{127}}$

$\overline{\theta^{(C)}} = 1/127$, $\overline{|\theta^{(C)}|} = 1217/127 = 9.5826$, $\sigma_\theta^{(C)} = 11.3133$

where the superscripts A, B, C, refer to the groups A, B, C respectively.

The interesting result is that the mean and variance of the autocorrelation or crosscorrelation for groups A, B, and C are independent of the group. The mean of the absolute value is approximately

$$\overline{|R|} \approx .07 \quad \text{less than} \quad 10\%$$

This value is not bad when one is not concerned about peak crosscorrelation. Since $\overline{R}^*$ is the same for Groups A, B, or C and since σ_R is the same also for Groups A, B, C, comparison of A, B, and C can only be done on basis of $|R|$ peak and $|R|$. On both these criteria group A becomes superior to the other groups. We call Group A a group with good crosscorrelation properties.

Sets of Sequences with Good Crosscorrelation Properties.

From Table 4 one could choose a set of 3 sequences with good crosscorrelation properties, i.e., all R_{13}, R_{15}, R_{35} belong to a set where the pairwise crosscorrelations are three valued as shown in Table 3 under Group A.

For four signals one could similarly choose 1, 3, 5, 8 with R_{13} R_{15} R_{18} R_{35} R_{38} and R_{58} all belonging to a set having the same crosscorrelation distribution.

For 5 signals one could choose 1, 3, 5, 8, 9. For 6 signals 1, 3, 5, 8, 9, 11 breaks down because (9, 11) belongs to Group B, but 1, 3, 5, 8, 9, 18 works.

For 7 signals one must consider many combinations but in general one can be sure that no set can be found of more than 9 signals such that for all i, j. i, j = 1, 2, . . . , ten or more θ_{ij} belong to Group A.

On the generation of a large set $(2^m + 1)$ of non-maximal PN sequences with good crosscorrelation properties. The crosscorrelation properties of the previously described sequences are not at all discouraging even for Groups B and C because the only difference is in the peak values which come with a very small probability, i.e., for Group B $\theta = -41$ occurs only once out of 127 possible times. Needless to say that the autocorrelation of each of the sequences is almost perfect (orthogonal), as shown earlier.

The only difficulty arises when one needs more than $\phi(L)/m$ sequences. One solution to this problem is to generate sequences S_i from two maximal sequences S_A and S_B of the same m as illustrated in Figure 2.

---

* $\overline{R} = \dfrac{\overline{\theta}}{127}$, $\sigma_R = \sigma_\theta / 127$.

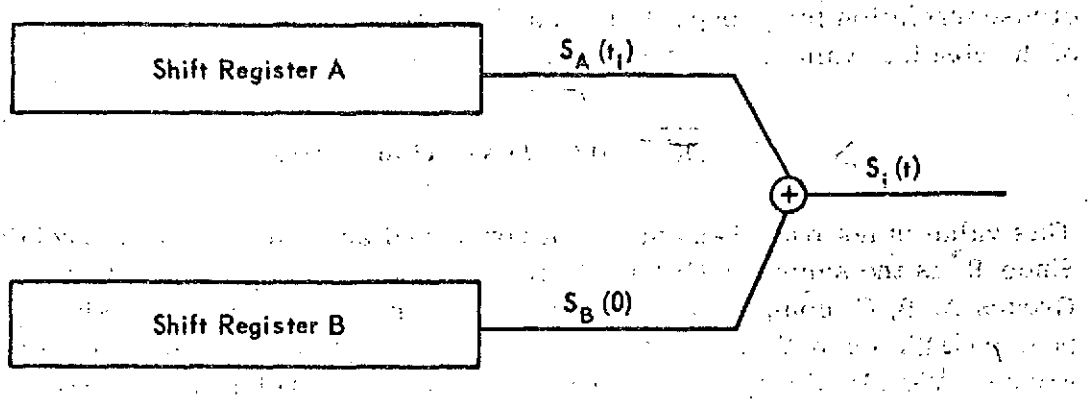

Figure 2

This configuration will generate* $2^m + 1$ non-maximal sequences of length $L = 2^m - 1$ whose autocorrelation and crosscorrelation for any two sequences will have the identical values (with identical frequencies) as the crosscorrelation of S_A and S_B . In other words by choosing S_A and S_B so that R_{AB} belongs to Group A, then S_i and S_j as generated by Figure 2 will be such that R_{ij} will also belong to Group A for all $i = 1, 2, \ldots\ldots 2^m + 1$ and $j = 1, 2, \ldots\ldots 2^m + 1$.

The Correlation of PN Sequences Without Limitation on the Length.

It was proven in Part 3 that if the correlation is a random variable for the case of a linear maximal PN sequence, the autocorrelation, had a mean equal to $(1/L)^2$ and a variance

$$\sigma_R^2 = \frac{(2^m - 1)^2 + 2^m - 2 - 1/(2^m - 1)}{(2^m - 1)^3}$$

which for large m can be approximated to

$$\sigma_R^2 \simeq \frac{1}{2^m - 1} = \frac{1}{L}$$

where L is the length of the sequence.

* See Appendix D

** One exception is the autocorrelation of 2 of these sequences $S_i = S_A \oplus 0 = S_A$ and $S_i = S_B + 0 = S_B$ which is $-1/(2^m - 1)$ for $\tau \neq 0$ and 1 for $\tau = 0$.

It has also been observed that the crosscorrelation of any two maximal PN sequences of the same degree (or length) has the same variance and mean as above.

The question that arises is: "What is the mean and variance of the autocorrelation or crosscorrelation when the sequence is not crosscorrelated for its entire length?"

a. Letting the segments be p bits along with $p \leq m$, the correlation of two p bit segments of a sequence S is

$$\theta(\tau) = \sum_{j=0}^{p} S_j(0)\, S_j(\tau)$$

by applying properties D and C

$$\theta(\tau) = [\#\text{ of 0's} - \#\text{ of 1's}] \text{ in } S_C$$

where

$$S_C = S(0) \oplus S(\tau) = S(\tau_i)$$

letting w denote the weight* of the p-tuplet then

$$\theta(\tau) = p - 2w$$

Since w is not known for each τ, it is treated as a random variable; once the probability density** function of w is found one can find $\overline{\theta}$ and $\overline{\theta^2}$. For each w, there are C_w^p p-tuplets since there are C_w^p ways of having w "ones" in p distinct (ordered) positions.

* The weight is equal to the number of 1's

** Since w is discrete, instead of the probability density we find the frequency of occurrence f_w

Obviously the frequency of a given distinct p-tuplet* in a maximal sequence of 0's and 1's is 2^{n-p}**. Therefore the frequency of a given w or correspondingly θ_w is

$$f_w = 2^{n-p} C_w^p$$

Then the expression for $\overline{\theta}$ becomes:

$$\overline{\theta} = \frac{1}{L} \sum_{i}^{p} \theta_i f_i = \frac{1}{L} \sum_{w}^{p} \theta_w f_w = \frac{p}{L} \sum_{w}^{p} 1 - \left(\frac{2w}{p}\right) f_w$$

$$= \frac{p}{L} \sum_{w}^{p} f_w - \frac{2}{L} \sum_{w}^{p} w f_w$$

$$= p - \frac{2}{L} \sum_{w}^{p} w \; 2^{n-p} \; C_w^p$$

$$= p - \frac{2^{m+1-p}}{L} \sum_{w}^{p} w \; C_w^p$$

From Appendix E

$$\sum_{w}^{p} w \; C_w^p = \frac{p}{2} \; 2^p$$

and

$$\overline{\theta} = p - \frac{2^{m+1-p}}{L} \frac{p}{2} 2^p = \frac{p}{L} [2^m - 1 - 2^m] = -\frac{p}{L}$$

consequently

$$\overline{R} = \frac{\overline{\theta}}{p} = -\frac{1}{L}$$

* For a Shift Register generated sequence the all zero p-tuplet has a frequency of $2^{m-p} - 1$ because the all zero m-tuplet is the only m-tuplet which is absent from the maximal sequence. However, in this discussion this fact will be neglected for the sake of simplicity with no considerable error.

** This is the amount of times that a distinct p-tuplet appears in an m-dimensional space over GF_2.

The standard deviation of θ, σ_θ^2, is be definition:

$$\sigma_\theta^2 = \frac{1}{L} \sum_w (\theta_w - \theta)^2 f_w = \frac{1}{L} \sum_w R_w^2 f_w - \bar{\theta}^2$$

the first term becomes

$$\frac{2^{m-p}}{L} \sum_w^p p \left(1 - \frac{2w}{p}\right)^2 C_w^p = \frac{2^{m-p}}{L} p \sum_w^p \left[C_w^p - \frac{4w}{p} C_w^p + \frac{4w^2}{p^2} C_w^p\right]$$

now

$$\sum_w^p C_w^p = \sum_w^p C_w^p \; 1^{p-w} \; 1^w = (1+1)^p = 2^p$$

from Appendix E

$$\sum_w^p w \, C_w^p = \frac{p}{2} \; 2^p$$

from Appendix F

$$\sum_w^p w^2 \, C_w^p = \frac{p}{2} 2^p + p(p-1) \, 2^{p-2}$$

$$= p \; 2^p \left[\frac{1}{2} + \frac{p-1}{4}\right]$$

The first term becomes

$$\frac{2^{m-p}}{L} p \left[2^p - 2 \cdot 2^p + \frac{4}{p} \; 2^p \left(1/2 + \frac{p-1}{4}\right)\right] = 2^m/L$$

then

$$\overline{\theta^2} = \frac{2^m}{L^2} - \frac{p^2}{L^2} = \frac{2^m (2^m - 1) - p^2}{L^2}$$

for large L

$2^m \approx L$ and $P/L^2 \approx 0$ and $\overline{\theta}^2 = 1$, and

$$\overline{R}^2 = \frac{1}{p} \overline{\theta}^2 = \frac{1}{p}.$$

If p is greater than m (with still linear sequences) these relations, although no longer true, may be considered as upper bounds for the following reasons.

If p - m = b, given the first m bits the remaining b bits of the p-tuplet are determined depending on the feedback connections of the shift register; furthermore there are only 2^m p-tuplets (not 2^p) which obviously makes some* p-tuplets inadmissible. The majority of the above inadmissible p-tuplets are the type whose weights is much different from the mean weight $\overline{w}$; (i.e. p-tuplets containing more than m consecutive 0's or 1's). Consequently the standard deviation should be smaller than the one found above.

Now if one assumes that the above inadmissible p-tuplets exist in the sequence but that their frequency is 2^{m-p} (which in this case is a fraction of unity) the equations of section 5 should still hold so far as the frequency of a distinct ordered p-tuplet is concerned. (These equations should not be considered an upper-bound) i.e. if only one p-tuplet out of the 2^{p-n} (p > n) is admissible we may say that on the average the frequency of a distinct p-tuplet is 2^{m-p} or $1/2^{p-m}$ (p > n) so that the frequency of a given w is still $2^{n-p}\ C_w^p$.

*2^{p-m}

REFERENCES

1. Morakis, J. C., "Shift Register Generators and Applications to Coding," X-520-68-133, April 1968

2. Gold, R., "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE IT 13 #4, p. 619

3. Peterson, W. W., "Error-Correcting Codes," MIT, Wiley

4. T. A. Dowling and R. McEliece, "Cross-Correlations of Reverse Maximal-Length Shift Register Sequences," JPL Space Programs Summary 37-53, Vol. III, pp. 192, 193.

APPENDIX A

This appendix is used to arrive at the formulation of the transition matrix A by treating the contents of the shift register as a state vector. The analysis has many gaps. For more rigorous analysis the reader is referred to [1].

Definition: A maximal pseudo-random sequence S_A is a sequence generated by a feedback shift register connected to divide by the primitive polynomial $P_A(x)$; the period is $2^n - 1$. $P_A(x)$ is of the form

$$P_A(x) = \sum_{i=0}^{n} h_i x^i \quad \text{with} \quad h_i = 0, 1 \quad \text{and} \quad h_0 = h_n = 1 \tag{1}$$

and it is the characteristic equation of the transition matrix A that gives the relationship between the state (contents) of the Shift register generator at some time t and another time $t + \tau$. If u(t) represents the contents of the shift register at time t then

$$u(t + \tau) = A^{\tau} u(t) \tag{2}$$

or

$$u(t + 1) = A\, u(t) \tag{3}$$

u(t) is an n-dimensional vector and if it is considered as an n-symbol segment of the sequence S_A then u(t + 1) will contain n - 1 of the symbols in u(t) and a new symbol which is a function of the n - 1 previous symbols as shown by the matrix A in the companion form.

$$\begin{bmatrix} u_1(t+1) \\ u_2(t+1) \\ u_3(t+1) \\ \cdot \\ \cdot \\ \cdot \\ u_{n-1}(t+1) \\ u_n(t+1) \\ \cdot \end{bmatrix} = \begin{bmatrix} 0\,1\,0\,0\,0\,0\,0\,\ldots\,0\;\;0 \\ 0\,0\,1\,0\,0\,\ldots\,0\;\;0 \\ 0\,0\,0\,1\,0\,\ldots\,0\;\;0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0\,0\,0\,0\,\ldots\,0\,0\,0\;\;1 \\ h_0 h_1 h_2 h_3 \ldots\ldots h_{0-2} h_{n-1} \end{bmatrix} \begin{bmatrix} u_1(t) \\ u_2(t) \\ \\ \\ \\ \\ \\ u_{n-1}(t) \\ u_n(t) \end{bmatrix} \tag{3a}$$

The above equation results in the following relationships

$$u_i(t+1) = u_{i+1}(t) \quad t = 1, 2, \ldots\ldots n-1 \tag{4}$$

and

$$u_n(t+1) = \sum_{i=0}^{n-1} h_i u_{i+1}(t) = \sum_{i=0}^{n-1} h_i u_i(t+1) \tag{5}$$

Since the last equation

$$u_n(t+1) = \sum_{i=0}^{n-1} h_i\, u_i\, (t+1) \tag{6}$$

is independent of time we can drop the time dependent thus resulting in the recursive formula

$$u_n = \sum_{i=0}^{n-1} h_i u_i \qquad (7)$$

which gives the nth symbol of the sequence in terms of the n previous symbols. It should be noticed that the h_i's of equation (1) are identical to those of equation (7).

APPENDIX B

ON THE ROOTS OF POLYNOMIALS OF A SPECIFIED PERIOD

This appendix is written in order to prove some interrelationships between roots of polynomials.

1. Let

$$P(x) = \sum_i h_i x^i$$

be a polynomial with coefficients from GF(2). Let α be a root of the polynomial P(x); then

$$P(\alpha) = \sum_i h_i \alpha^i = 0$$

Now consider

$$[P(\alpha)]^2$$

$$[P(\alpha)]^2 = \left[\sum_i h_i \alpha_i \right]^2 = 0$$

but

$$\left[\sum_i h_i \alpha^i \right]^2 = \sum_i h_i^2 (\alpha^i)^2 \oplus 2 \sum_i \sum_j h_i h_j \alpha^{i+j}$$

$$= \sum_i h_i \alpha^{2i} + 0 = P(\alpha^2)$$

because

$$h_i^2 = h_i \quad \text{in GF (2)} \quad \text{and} \quad 2 = 0 \mod 2$$

Thus

$$P(\alpha^2) = [P(\alpha)]^2 = 0$$

We conclude that $\beta = \alpha^2$ is also a root of P (x). In general if $k = 2^{\ell}$

$$[P(\alpha)]^k = P(\alpha^k) = 0$$

because

$$\left[\sum_i h_i \alpha^i\right]^k = \sum_i h_i \alpha^{ik} + C_j^k \quad \text{(other terms)}$$

but

$$C_j^k = \frac{k!}{(k-j)!j!} = 0 \mod 2 \quad \text{for} \quad j \neq k.$$

In general if a polynomial has a root α then $\alpha^{2^{\ell}}$ is also a root. When $2^{\ell} > 2^m - 1$ then 2^{ℓ} is taken mod $2^m - 1$ which is the period of the root. Example for $m = 5$ $2^m - 1 = 31$. If $\beta = \alpha^{11}$ is a root then $\beta^{2^{\ell}}$ are also roots of the polynomial; then the roots are:

$$\alpha^{11},\ \alpha^{22},\ \alpha^{44 \bmod 31} = \alpha^{13},\ \alpha^{26} \quad \text{and} \quad \alpha^{52 \bmod 31} = \alpha^{21}$$

thus any of α^{11}, α^{22}, α^{13}, α^{26} or α^{21} satisfy the same polynomial of degree 5.

2. The Roots of the Reverse Polynomial.

The primitive characteristic polynomials can be found in Tables. Some of the tables contain only half of the primitive polynomials. The other half are the ones representing the reverse sequences and can be obtained by finding the polynomials due to $\beta^{2^{m-1}} - 1$ for each β. Proof: Let β be the root of an arbitrary primitive polynomial.

$$P(x) = x^m + x^p + x^q + x^{\ell} + 1$$

then

$$P(\beta) = \beta^u + \beta^p + \beta^q + \beta^\ell + 1 = 0$$

Now consider the polynomial due to the reverse sequence*

$$P_R(x) = x^u + x^{n-p} + x^{n-q} + x^{n-\ell} + 1$$

We shall test the root

$$\beta^{2^{m-1}-1} = \beta^{-2^{m-1} \bmod 2^m - 1}$$

on $P_R(x)$ and more generally we shall test the root β^{-2^k} on $P_R(x)$ k = 0, 1, 2, ... m - 1 because β^{-1}, β^{-2}, β^{-4}, ... β^{-2^1}, ... $\beta^{-2^{m-1}}$ are roots of the same polynomial ($\beta^{-2^m} = \beta^{-2^m \bmod 2^m - 1} = \beta^{-1}$). Thus the polynomial P_R is satisfied by β^{-1}; it is also satisfied by the above mentioned roots.

$$P_R(\beta^{-1}) = \frac{1}{\beta^n} + \frac{1}{\beta^{n-p}} + \frac{1}{\beta^{n-q}} + 1$$

$$= \beta^{-n} \left[1 + \beta^p + \beta^q + \beta^\ell + \beta^n\right]$$

but the equation in the brackets is zero ($P(\beta)$). Thus

$$P_R(\beta^{-1}) = \beta^{-n} P(\beta) = 0 \quad \text{QED.}$$

*See [1] for proof.

Consequently β^{2^k} is a root of $P_R(x)$

for k = 0, 1, ... m - 1. Thus the positive exponents of the roots that satisfy $P_R(x)$ are

$$2^m - 1 - 2^k, \quad k = 0, 1, 2, \ldots, m-1,$$

The smallest power of β being

$$2^m - 1 - 2^{m-1} = 2^{m-1} - 1 \quad (\text{for } k = m-1). \quad \text{QED.}$$

APPENDIX C
CROSSCORRELATION GROUPS AND ROOTS OF SEQUENCES

This appendix explains the grouping of sequences S_b for S_a equal to one of the 18 sequences. The first part of Table 4 gives the sequences in Group A and in Group B when S_a is sequence #1 (its reverse is #2) and it is rewritten for convenience.

S_a = Sequence #1 (root is α)

GROUP A = Sequence #'s 3, 5, 8, 9, 11, 12, 13, 14, 16, 18.

GROUP B = Sequence #'s 4, 6, 7, 10, 15, 17

Another way of identifying the sequences is by using the exponent of one of their roots. Since each sequence has 7 roots we shall use the smallest of the 7 exponents (the first entry of the second column of Table 2). Thus the sequence number and root identification become the pairs (sequence #, root exponent) = (1,1), (2,63), (3,3), (4,31), (5,5) (6, 47), (7,7), (8,15), (9,9), (10,55), (11,11), (12,39), (13,13), (14,23), (15,19), (16,27), (17,21), (18,43).

On the root identification basis, when the root of S_a is α (root exponent = 1) Group A becomes the sequences whose roots have exponents 3, 5, 15, 9, 11, 39, 13, 23, 27, 43 and similarly Group B becomes

B = 31, 47, 7, 59, 19, 21

Group C consists of the reverse sequence only with root* α^{63}. Notice that the sequence whose roots is $\alpha^{17} = \alpha^{9}$ mod 127 is in group A as predicted by Gold [2]. Notice also that this is not the only sequence whose crosscorrelation with sequence #1 is less than or equal to 17. Nine more sequences have identical crosscorrelation values and frequencies.

Now consider the second entry, i.e. sequence #2 with root identification 63. Setting $\alpha^{63} = \beta$ the root of sequence #2 let us find β^3, β^5, β^{15}, β^9, β^{11}, β^{39}, β^{13}, β^{23}, β^{27} and β^{43}. Notice that the exponents of the above roots are the exponents of the α's in case 1 for Group A.

*See Appendix B

$\beta^3 = (\alpha^{63})^3 = \alpha^{31} \longleftrightarrow$ sequence # 4

$\beta^5 = (\alpha^{63})^5 = \alpha^{61} \longleftrightarrow$ sequence # 6

$\beta^{15} = \alpha^{56} \longleftrightarrow$ sequence # 7

$\beta^9 = \alpha^{59} \longleftrightarrow$ sequence # 10 has root β^{17}

$\beta^{11} = \alpha^{58} \longleftrightarrow$ sequence # 12

$\beta^{39} = \alpha^{11} \longleftrightarrow$ sequence # 11

$\beta^{13} = \alpha^{57} \longleftrightarrow$ sequence # 14

$\beta^{23} = \alpha^{52} \longleftrightarrow$ sequence # 17

$\beta^{27} = \alpha^{50} \longleftrightarrow$ sequence # 15

$\beta^{43} = \alpha^{42} \longleftrightarrow$ sequence # 17

but sequences #4, 6, 7, 10, 12, 11, 14, 17, 15, 18 form Group A for sequence 2 as seen in Table 2. This result shows a possibility that the crosscorrelation Group of values have a dependence on the roots of the sequences. Thus if α is a root of the sequence S_α then Group A consists of sequences whose roots are α^{ℓ_A} with ℓ_A given by

$$\ell_A = 3,\ 5,\ 15,\ 9,\ 11,\ 39,\ 13,\ 23,\ 27,\ 43$$

and group B consists of sequences whose roots are α^{ℓ_B} with ℓ_B given by

$$\ell_B = 31,\ 47,\ 7,\ 55,\ 19,\ 21$$

similarly

$$\ell_C = 63$$

As we have seen if S_α is sequence #2 with root β ($\beta = \alpha^{63}$) then to find group A all we need do is raise β to the powers ℓ_A as we have done, with results identical to the ones in Table 2, part 2, Group A. Thus for Group B raise β to ℓ_A and identify the corresponding sequences.

$$\beta^{31} = (\alpha^{63})^{31} = \alpha^{48} \longleftrightarrow \text{sequence \#} \quad 3$$

$$\beta^{47} = (\alpha^{63})^{47} = \alpha^{40} \longleftrightarrow \text{sequence \#} \quad 5$$

$$\beta^{7} = (\alpha^{63})^{7} = \alpha^{15} \longleftrightarrow \text{sequence \#} \quad 8$$

$$\beta^{55} = (\alpha^{63})^{55} = \alpha^{36} \longleftrightarrow \text{sequence \#} \quad 9$$

$$\beta^{19} = (\alpha^{63})^{19} = \alpha^{54} \longleftrightarrow \text{sequence \#} \quad 16$$

$$\beta^{21} = (\alpha^{63})^{21} = \alpha^{53} \longleftrightarrow \text{sequence \#} \quad 18$$

The sequences are #'s 3, 5, 8, 9, 16, and 18 and they agree with the Group B entry in part 2 of Table 2. (Of course Group C is sequence 1; check:

$$\beta^{63} = (\alpha^{63})^{63} = \alpha^{32} \longleftrightarrow \text{Sequence \#1).}$$

Let us derive now the Correlation Groups for the 6th sequence. Let the root of sequence #6 be $\gamma = \alpha^{47}$ Table C gives the information on the powers of γ, α, and corresponding sequence number for Groups A, B, and C. It can be seen that the numbers at the third column correspond to the ones for Groups A and B in Table 4 and Group C is sequence 5 as expected. The remaining entries of Table 4 could be derived in this manner.

TABLE C

$\gamma = \alpha^{47} \longleftrightarrow$ sequence #6

	Exponent of γ	Exponent of α	Sequence #
	3	3(47) = 14 mod 127	7
	5	5(47) = 108 mod 127	16
	15	15(47) = 70 mod 127	13
	9	9(47) = 42 mod 127	17
	11	= 9 mod 127	9
Group A	39	= 55 mod 127	10
	13	= 103 mod 127	4
	23	= 65 mod 127	3
	27	= 126 mod 127	2
	43	= 116 mod 127	12
	31	= 60 mod 127	8
	47	= 50 mod 127	15
	7	= 75 mod 127	14
Group B	59	= 106 mod 127	18
	19	= 4 mod 127	1
	21	= 98 mod 127	11
Group C	63	= 40 mod 127	5

APPENDIX D

This appendix is devoted to the development of certain sequences S_i of Fig. D1 with identical crosscorrelation properties as the original two generator sequences. Before proceeding we repeat four important properties that will be used in the course of the proofs.

A Sequence of period L can be viewed as a sequence of L states (n-dimensional vectors $L = 2^n - 1$ for binary).

Property 1. A maximal binary sequence will occupy all $2^n - 1$ non-zero states before it starts repeating.

Property 2. (Balance property). The number of 1's in a maximal sequence exceeds the number of 0's by 1.

Thus the number of zeros of a maximal sequence is equal to $2^{n-1} - 1$ and the number of 1's is equal to 2^{n-1}.

Property 3. (The Shift-and-add property).

When a maximal sequence is first shifted by t bits and then added to itself the resulting sequence is the same sequence delayed by some time t_1 i.e.

$$S_A(0) + s_A(t) = s_A(t_1) \quad t \neq 0^*$$

This property becomes obvious from the following argument. A shift register generated sequence described by equation (7) in Appendix A in a linear process. Thus if the elements of $S_A(0)$, u_n obey the equation

$$u_n(0) = \sum_{i=0}^{n-1} h_i u_i(0)$$

then the elements of $S_A(t)$ obey the equation

*All additions are mod 2 unless they result in some statistic R or θ and their functions.

$$u_n(t) = \sum_{i=0}^{n-1} h_i u_i(t)$$

thus the elements of the sequence $[S_A(0) + S_A(t)]$ are

$$v_n = u_n(0) + u_n(t) = \sum_{i=0}^{n-1} h_i [u_i(0) + u_i(t)] = \sum_{i=0}^{n-1} h_i v_i$$

where

$$v_i = u_i(0) + u_i(t)$$

Since v_n obeys the same equation as u_n (the same set of h_i's) the sequence whose element is v_n is the same as S_A except for a delay, if S_A is maximal. (If S_A is non-maximal then v_n may be another non-maximal sequence obeying the same recursive equations).

A transformation that changes the correlation function to the difference of the numbers of 1's and zeros in a sum sequence. Consider two sequences S_A and S_B. The correlation of S_A and S_B as a function of t is defined as

$$R_{AB}(t) = \frac{1}{L} \sum_{i=1}^{L} S_A(0) \cdot S_B(t)$$

defining

$$\theta_{AB}(t) = L R_{AB}(t)$$

$\theta_{AB}(t)$ turns out to be the inner product of S_A and S_B (t). Thus

Thus

$$\theta_{AB}(t) = \theta [S_A(0), S_B(t)] = \sum_i a_i \cdot b_{i+t}$$

where

$$S_A = [a_1, a_2, a_3 \ldots .], \quad S_B = [b_1, b_2, b_3 \ldots .] \quad \text{and} \quad a_i, b_j = -1, 1$$

if $a_i, b_j = 1, 0$ then one can apply the following transformation

$$1 \rightarrow 0 \quad -1 \rightarrow 1 \quad \text{resulting in} \quad \bullet \rightarrow \oplus \quad (\text{mod 2 addition})$$

(Another way to look at this is in terms of agreements and disagreements). The summation sign adds all agreements (1's) and subtracts the disagreements (-1's); now that we transformed the 1's to 0's and the -1's to 1's, we must add the zeros and subtract the ones of the sequence resulting from the modulo 2 addition of $S_A(0)$ and $S_B(t)$. The reason for this transformation is the fact that very often we are able to determine the counts of 0's and 1's of a sequence resulting from a mod 2 addition of two other sequences, without going through the mechanics of adding bit by bit. Subsequently this count of 0's and 1's will readily enable us to determine the correlation of S_A and $S_B(t)$. If

$$S_C = S_A(0) + S_B(t)$$

then

$$\theta_{AB}(t) = [\text{the number of zeros in } S_C] - [\text{the number of ones in } S_C]$$

By using the above properties we shall now determine the autocorrelation function $\theta_{AA}(t)$ of maximal shift register generated sequences. Letting S_A be this sequence

$$\theta_{AA}(t) = (\#\text{ of zeros in } S_C) - (\#\text{ of ones in } S_C)$$

where

$$S_C = S_A(0) \oplus S_A(t)$$

by using the shift-and-add property for the maximal sequence S_A

$$S_C = S_A(t') \quad \text{for} \quad t' \neq 0$$

Furthermore using the balance property for maximal sequences

$$[\#\text{ of zeros in } S_A(t')] - [\#\text{ of 1's in } S_A(t')] = -1$$

resulting in

$$\theta_{AA}(t) = -1 \quad \text{for} \quad t \neq 0$$

or

$$R_{AA}(t) = \frac{-1}{2^n - 1}$$

for $t = 0$

$$S_C = S_A(0) + S_A(0) = 2\,S_A(0) = 0$$

resulting in the all zero sequence with $2^n - 1$ zeros; then

$$\theta_{AA}(0) = [\#\text{ of zero in } S_C] - [\#\text{ of ones in } S_C] = 2^n - 1 - 0 = 2^n - 1$$

and

$$R_{AA}(0) = (2^n - 1)/(2^n - 1) = 1$$

Suppose now that we generate sequences S_i by the polynomial P(X) which is the product of $P_A(x)$ and $P_B(x)$, the primitive polynomials of degree n which were defined previously.

$$P(x) = P_A(x) \cdot P_B(x)$$

This is equivalent to taking $S_A(t)$ and $S_B(0)$ and mod 2 add them (bit by bit)

$$S_i(0) = S_A(t_i) \oplus S_B(0)$$

This can be accomplished by the configuration of Figure 1.

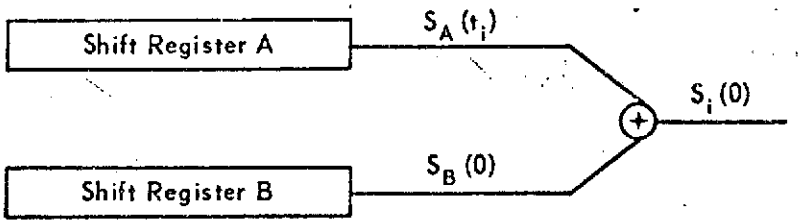

Figure D 1

It will now be shown that the auto and crosscorrelation of the sequences S_i generated by the technique of Figure 1 takes on the same values as the cross-correlation of S_A and S_B. The crosscorrelation of two sequences S_i and S_j $(i \neq j)$ is

$$\theta_{ij}(t) = \theta[S_i(0) \oplus S_j(t)] = \#\text{ of 0's in } S_k - \#\text{ of 1's in } S_k$$

where

$$S_k = S_i(0) \oplus S_j(t).$$

Substituting for S_i and S_j

$$S_i(0) = S_A(t_i) \oplus S_B(0).$$

$$S_j(t) = S_A(t_j + t) \oplus S_B(t)$$

$$S_k(0) = S_A(t_i) \oplus S_A(t_j + t) \oplus S_B(0) \oplus S_B(t)$$

$$= S_A(\ell_1) \oplus S_B(\ell_2).$$

Now going backwards the numbers of zeros and ones in S_k is equal to the numbers of zeros and ones in $S_A(\ell_i) + S_B(\ell_2)$; thus

$$[\#\ 0\text{'s in } S_k(0)] - [\#\ \text{of } 1\text{'s in } S_k(0)] = \theta[S_A(\ell_1), S_B(\ell_2)]$$

or

$$\theta_{ij}(t) = \theta_{AB}(\ell_1 - \ell_2)$$

thus the crosscorrelation of S_i and S_j is equal to the crosscorrelation of S_A and S_B at some other time delays. Let us now examine the upper bound of the autocorrelation of S_i

$$\theta_{ii}(t) = \theta[S_i(0), S_i(t)] = [\#\ \text{of } 0\text{'s in } S_{ii}] - [\#\ \text{of } 1\text{'s in } S_{ii}] \text{ and } t \neq 0$$

where $S_{ii} = S_i(0) + S_i(t)$. By making the proper substitution

$$S_{ii} = S_A(t_i) + S_B(0) \oplus S_A(t_i + t) \oplus S_B(t)$$

$$= S_A(t_i) + S_A(t_i + t) \oplus S_B(0) + S_B(t) \quad t \neq 0$$

$$= S_A(\ell_3) + S_B(\ell_2)$$

and

$$\theta_{ii}(t) = \theta_{AB}(\ell_3 - \ell_2)$$

Yielding the same results as before. Thus both autocorrelation and cross-correlation of the sequences S_i generated by the products of the primitive polynomials $P_A(X)$ and $P_B(X)$ are equal to some crosscorrelations of S_A and S_B.

For the case where S_j, the interfering sequence, is really a linear sum of other sequences, (but not S_i the primary sequence), the crosscorrelation then still has the same values as the crosscorrelation of S_A and S_B. This will be shown in the sequel

let $$S_j = \sum_{\ell \neq i} S_\ell(t_\ell) \mod 2$$

The sum sequence S_K becomes

$$S_K = S_i \oplus \sum_{\ell \neq i} S_\ell(t_\ell) \mod 2$$

but $$S_i = S_B(0) \oplus S_A(t)$$

and each $S_\ell(t_\ell)$ is the sum of some $S_B(t_{\ell_1})$ and $S_A(t_{\ell_2})$ thus

$$S_K = S_A(t) \oplus S_B(0) + \sum_{\ell \neq i} \left[S_B\left(t_{\ell_1}\right) \oplus S_A\left(t_{\ell_2}\right) \right] \mod 2$$

$$= \sum_{\ell} S_B\left(t_{\ell_1}\right) \oplus \sum_{\ell} S_A\left(t_{\ell_2}\right) \mod 2$$

Now by using the shift and add property

$$\sum_{\ell} S_A\left(t_{\ell_2}\right) = S_A(t_3)$$

and

$$\sum_{\ell} S_B\left(t_{\ell_1}\right) = S_B(t_4)$$

$$S_K = S_A(t_3) \oplus S_B(t_4). \quad \text{QED}$$

APPENDIX E

$$\sum = \sum_{w}^{p} w\, C_w^p = \sum_{w}^{p} w \binom{p}{w}$$

$$= \sum_{w=0}^{p/2} w \binom{p}{w} + \sum_{w=p/2+}^{p} w \binom{p}{w}$$

replace w in the second term by p - k; then the second term becomes

$$\sum_{k=p/2-}^{0} (p-k) \binom{p}{p-k} = \sum_{k=0}^{p/2} (p-k) \binom{p}{k}$$

since

$$\binom{p}{k} = \binom{p}{p-k} = \frac{p!}{k!\,(p-k)!}$$

Consequently $\sum$ becomes

$$= \sum_{w=0}^{p/2} w \binom{p}{w} + \sum_{k=0}^{p/2} (p-k) \binom{p}{k} \quad \text{replacing k by w}$$

$$= \sum_{w=0}^{p/2} w \binom{p}{w} + \sum_{w=0}^{p/2} (p-w) \binom{p}{w}$$

$$= \sum_{w=0}^{p/2} [w + (p-w)] \binom{p}{w} = p \sum_{w=0}^{p/2} \binom{p}{w} \qquad \text{(A-1)}$$

Now

$$\sum_{w=0}^{p} \binom{p}{w} = \sum_{w=0}^{p} \binom{p}{w} 1^w \cdot 1^{p-w} = (1+1)^p = 2^p \qquad \text{(A-2)}$$

since (p/w) is symmetrical about w = p/2

$$\sum_{w=0}^{p/2} \binom{p}{w} = \frac{1}{2} \sum_{w=0}^{p} \binom{p}{w} = \frac{1}{2} 2^p$$

Substituting the above result in equation A-1

$$\sum = p \sum_{w=0}^{p/2} \binom{p}{w} = p \frac{1}{2} 2^p = \frac{p}{2} 2^p ,$$

APPENDIX F

To find

$$\sum_{i}^{p} i^2 \binom{p}{i} ; \quad \text{letting} \quad i^2 = i(i-1) + i$$

the above expression is equal to

$$\sum_{i}^{p} i(i-1) \binom{p}{i} + \sum_{i}^{p} i \binom{p}{i} \quad *$$

since the first two terms are 0, (for i = 0, 1)

$$= \sum_{i=2}^{p} i(i-1) \binom{p}{i} + 2^p \frac{p}{2}$$

$$= \frac{p}{2} 2^p + \sum_{i=2}^{p} i(i-1) \frac{p!}{i!\,(p-i)!}$$

$$= \frac{p}{2} 2^p + p(p-1) \sum_{i=2}^{p} \frac{(p-2)!}{(i-2)!\,(p-i)!}$$

let i - 2 = k

---

* $\sum_{i}^{p} i \binom{p}{i} = \frac{p}{2} 2^p$ from Appendix E

$$\sum_{i}^{p} i^2 \binom{p}{i} = \frac{p}{2} 2^p + p(p-1) \sum_{k=0}^{p-2} \frac{(p-2)!}{k!(p-k-2)!}$$

$$= \frac{p}{2} 2^p + p(p-1)\, 2^{p-2} \quad *$$

* also from Appendix E